



mptcp: pm: in-kernel: always mark signal+subflow endp as used

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-23321
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:28 UTC
Updated	2026-04-23 21:05:32 UTC

Description In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: in-kernel: always mark signal+subflow endp as

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: NVD-CWE-Other

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected d93cf38fad9f66397093432b8917971a92ee0146 c5c877e140e5f46023a74a51e577ce5edd0a4be7 git
CNA	Linux	Linux	affected 64815ba15880ce5f99df075fa4104fef170ac7e5 05799c2f1ca5eb13d65764dda688d02021b65e06 git
CNA	Linux	Linux	affected 85df533a787bf07bf4367ce2a02b822ff1fba1a3 67f34ab318807989b57dfdb0f79e2d4e57018290 git
CNA	Linux	Linux	affected 85df533a787bf07bf4367ce2a02b822ff1fba1a3 a64aa7db39392add5be09dffaedbf1f0ce5554df git
CNA	Linux	Linux	affected 85df533a787bf07bf4367ce2a02b822ff1fba1a3 198824ccfa64ffe9bd918bf99c939bd8170a4a4d8 git
CNA	Linux	Linux	affected 85df533a787bf07bf4367ce2a02b822ff1fba1a3 579a752464a64cb5f9139102f0e6b90a1f595ceb git
CNA	Linux	Linux	affected 0f21cc29bc13e86512621727a4388c8a7ad2716b git
CNA	Linux	Linux	affected 6.11
CNA	Linux	Linux	unaffected 6.11 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/198824ccfa64ffe9bd918bf99c939bd8170a4a4d8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/67f34ab318807989b57dfdb0f79e2d4e57018290	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/05799c2f1ca5eb13d65764dda688d02021b65e06	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/579a752464a64cb5f9139102f0e6b90a1f595ceb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c5c877e140e5f46023a74a51e577ce5edd0a4be7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/a64aa7db39392add5be09dffaedbf1f0ce5554df	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)